The Growth and Development of Public Key Cryptography

By
Clifford Cocks
Old Style Cryptography
Key Management in the 60s

- Explosion in the need for secure comms
- Key management very labour intensive
- Real concerns of security as net sizes get bigger

Solution: Do some research into more efficient methods
James Ellis
Encryption

■ It is generally regarded as self-evident that….

■ …it is necessary to have some initial information….

■ ….kept SECRET from the interceptor
Non-Secret Encryption

- Secure messages sent even though
  - the method of encipherment and
  - all transmissions
- are known to the interceptor
For a short wire connection:
Recipient adds Random noise to the line which (since he knows it) he can subtract again
Model NSE System

Sender

M2

Message

Enciphered key

M1

Enciphered Message

Recipient

M3

Deciphered Message

Key
Existence Proof

M1, M2 and M3 are huge look-up tables

Say -
M1 is a $2^{100}$ long 1 dimensional table

M2 is a $2^{100} \times 2^{100}$ 2 dimensional table

M3 is the appropriate 2 dimensional table to make the whole thing work
Table Construction

\[ M3[M2[P,M1[K]],K] = P \]
The Search is on!

■ It is easy to see that such machines can be represented as look-up tables.

■ The question is, can we find realisable machines with the required functionality (ie computable functions with the right properties)?
Early Reactions

1969 Chief Mathematician comments
- No reason in principle against the scheme
- but can’t think of implementation
- impressed by James’ ingenuity
- but uncertain how to take advantage of it

1970 - 1973 Several studies by mathematicians and engineers
But no useful results!
Breakthrough

Tunnel vision

Ellis Model

Solution

Nov 1973  1st practical solution
Cocks Implementation

Message = C

Enciphered Message = $D = C^{N} \mod N$

Deciphered Message = C

Key = P, Q

M2

Enciphered key

N = P Q

M1

M3

Sender

Recipient

Cocks Implementation

Message = C

Enciphered Message = $D = C^{N} \mod N$

Deciphered Message = C

Key = P, Q

M2

Enciphered key

N = P Q

M1

M3

Sender

Recipient
Shift Registers

- Used as components of many cryptologics of the time
- Distance Problem: Find number of steps between fills
- Natural representation as Finite Fields
Williamson’s 1st Method

January 1974

Message a: Fill of shift register of cycle length p

Sender
Random k

b = a**k

c = b**l = a**kl

d = c**K = a**l

Receiver
Random l

a = d**L
Williamson’s 2nd Method

Autumn 1974, written up August 1976

Sender

X**a

Recipient

X**b

Both can calculate X**ab

same as Diffie Hellman
Reactions to Real NSE

- CESG investigates implementation
  - Williamson preferred for engineering reasons
  - Concern about authentication
- 1970’s technology not up to the job
- Debate on ‘To patent or Not to patent’
Jan 1976  ‘Multiuser Cryptographic techniques’
- introduces PKC but no example or existence proof
- Ellis: ‘They are where I started in 1969’
- shows Ellis solution to Authentication problem

Nov 1976  ‘New Directions in Cryptography’
- Williamson 2nd Method
Rediscovery II (RSA)

Apr 1977  ‘A method for obtaining Digital Signatures and Public-key Cryptosystems’
What Then?

- Developing Theory
  - New Attacks
  - Mathematical Rigour
  - New Primitives

- Practical Uses
  - Cryptographic Products
  - Technology needed to catch up
  - Standards Emerge
A hard mathematical problem does not guarantee a secure cryptosystem.
Merkle & Hellman (1978): the subset sum problem

Given $S$, $\{M_i\}$

finding $b_i \in \{0,1\}$ such that $\sum b_i M_i = S$

is hard

but

if $M_k > \sum M_i$ (superincreasing)

it is easy
KNAPSACKS II

Hide the superincreasing sequence

$N, L, \{M_i\}$ is the secret key

$\{K_i = L \cdot M_i \mod N\}$ is the public key

To encrypt $\{b_i\}$

compute $S = \sum b_i K_i$ (so finding $b_i$ is hard)

To decrypt

$L^{-1} S \mod N = \sum b_i M_i \mod N$ (so finding $b_i$ is easy)
Shamir Crypto'82:

$M_1, M_2, \ldots$ are very small,

$K_i = L M_i \mod N$ and so for many $i$,

- $(L^{-1} \mod N) \cdot K_i$ is close to a multiple of $N$
- $K_i \cdot \left( \frac{L^{-1} \mod N}{N} \right)$ is close to an integer

Can use Lenstra's smallest vector in lattice methods to get approximation to $(L^{-1} \mod N)/N$
Adi Shamir, Ron Rivest, Len Adleman, Ralph Merkle, Martin Hellman, and Whit Diffie receive an award from IEEE at Crypto 2000
Goldwasser & Micali 1984
Security provably equivalent to quadratic residuosity.

Alice: \(N = PQ\) c s.t. \((c/P)=(c/Q)=-1\)

Bob: To send \(m \in \{0,1\}\)

Choose random \(y\)

Send \(y^2 c^m \pmod{N}\)
Security Proofs

- Theory now well developed
  - Fundamental part of subject
- Allows for clarity
  - What security properties are claimed
  - What mathematical/algorithmic primitives underly security?
- Needed for cryptosystem to be accepted
Developing Theory

Elliptic Curves

Neal Koblitz, Victor Miller 1985

\[ Y^2 = X^3 + AX + B \]

Defines group structure on points
Elliptic Curves

Neal Koblitz, Victor Miller 1985

\[ Y^2 = X^3 + AX + B \] on Finite Field

Defines finite group structure on points

- Alternative group for Diffie-Hellman
- \( N \) bits of security require only 2\( N \) bits of key
- much shorter transmissions than other methods
Products

■ Experimental Hardware ~1980
  – Sandia, MIT

■ Commercial Products from ~1985
  – Cylink CY1024
  – Racal Datacryptor
  – STU III
Software Era – Internet Growth

Internet Users Worldwide 1995-2007
Software Era - PGP

- Published 1991 by Phil Zimmerman
- Email encryption and signatures
- Introduces “web of trust” to manage public keys
Standards & Protocols

■ X.509 Certificates ISO 1988
■ PKCS RSA Data Security 1991 on
■ DSA Signature Algorithm 1991
■ SSL Netscape 1994
■ IPSec 1995
■ SMIME RSA Data Security 1995
■ Now IETF lead on standards
Public Key Attacks

- Low exponent
  - encrypt Hastad 1985
  - decrypt Wiener 1990
  - non-random padding Coppersmith 1995

Moral: Beware of small exponents
Public Key Attacks

Low exponent Coppersmith 1995

Polynomial of degree $k$: $p(x) = 0 \mod N$
has root $x_0$ where $|x_0| < N^{(1/k)}$

Then short vector in lattice methods find $x_0$ quickly

Fixed padding and low exponent:
$y = [\ast\ast\ast r_1, r_2, \ldots, r_m, \ast\ast\ast] = ar + b$

See $y^e = (ar + b)^e \mod N$
Public Key Attacks

Timing attacks

Kocher 1996

To compute $y^x \mod N$:

Set $R \leftarrow 1$, $z \leftarrow y$ then iterate:

If bit $i$ of $x = 1$:

$R \leftarrow (R \cdot z) \mod N$

$z \leftarrow z^2 \mod N$

Time to do modular multiplication may depend on $z$, $R$

Lots of samples: recover $x$ bit by bit

Moral: Blind the calculation
Public Key Attacks

Quantum Computation
- Shor's Algorithm 1994
- unitary operation on $2^n$ states with $n$ qbits
- Fourier Transform is a unitary operation
- at end of calculation sample one state by amplitude
- Can use this to break RSA and Diffie Hellman
Public Key Attacks

Quantum Computation

– Shor's Algorithm 1994

Calculate $x^a \mod N$ for $a = 1, \ldots, M$ and $M \sim N^2$

Observe $x^a$, now have set of values $a = a_0 \mod \Phi(N)$

Perform Fourier transform on $a$ values to recover $\Phi(N)$
Continuing Developments

- Pairings
- Identifier Based Cryptography
Identifier Based Cryptography

Bob’s Public Key derived from his identity
Alice encrypts with no need for directory
Bob gets his Private Key from a Trusted Authority

Shamir 1984
Identifier Based Cryptography

History

- Concept Proposed by Shamir 1984
- False starts: e.g. Tanaka 1987
- Expensive Scheme: Maurer 1991
- Pairings method: Boneh & Franklin 2001
- Improved QR method: Boneh Gentry & Hamburg 2007
Weil Pairing

■ E Elliptic curve over $F_q$
  – $e$ maps $E \times E \rightarrow F_{q^k}$
  – $e(A+B,C) = e(A,C) \cdot e(B,C)$
  – $e(A,B+C) = e(A,B) \cdot e(A,C)$

■ Originally used to attack proposed curves

■ Limited sets of “Pairing Friendly” curves
IDPKC from the Weil Pairing

Trusted Authority: secret: $x$

global: elliptic curve $E / F_p$

bilinear map $e: E \times E \rightarrow F_p^2$

Alice: $x \cdot IDA$

Bob: $x \cdot IDB$

Maps identities to points in $E$

Boneh & Franklin '01
Implementation Challenge: Make PKI work (better)